

Serial No.: 09/743,653  
Customer No. 24498

RECEIVED  
CENTRAL FAX CENTER  
RCA 89131  
AUG 09 2007

### REMARKS

The Office Action mailed February 6, 2007 has been reviewed and carefully considered. Claim 1 has been amended. Claims 1-4, 6 and 15-17 are currently pending. Claims 7-14 were previously withdrawn from consideration. No new matter has been added.

### Rejections under 35 U.S.C. §103(a)

Claims 1-4 and 15-17 currently stand rejected under 35 U.S.C. §103(a) as being unpatentable over United States Patent No. 5,144,663, to Kudelski (hereinafter, "Kudelski") in view of United States Patent No. 5,870,474, to Wasilewski (hereinafter, "Wasilewski"). The Applicant respectfully traverses the Examiner's rejection of claims 1-4 and 15-17, and respectfully requests reconsideration of the Examiner's rejection in light of the amendments and following comments.

The Examiner has stated that the combination of Kudelski and Wasilewski may be combined to render claims 1-4 and 15-17 obvious. The Applicant respectfully asserts that Kudelski, and Wasilewski, whether taken singly, or in any combination, fail to render obvious at least the claim 1 element of "decrypting said access information in a conditional access module using a private key associated with the shared public key, *wherein the private key is shared among a plurality of subscribers.*" When addressed individually, Kudelski and Wasilewski both fail to show, or even suggest, any element remotely similar to, or suggestive of, sharing the private key among a plurality of subscribers. Furthermore, the combination of Kudelski and Wasilewski further fails to teach, suggest, or render obvious in any way, at least the claim 1 element of decrypting with a private key, "wherein the private key is shared among a plurality of subscribers."

Referring now to the references individually, the Examiner has cited Wasilewski as teaching a system "where a public key system is used for encrypting access information (see, for example, column 8, lines 31-37) and where a public key is shared by a plurality of service providers." (See page 3, second paragraph of the Office Action of February 6, 2007).

However, the Applicant respectfully draws the Examiner's attention to column 10, lines 13-14 of Wasilewski, which states that "According to the present invention, each STU [set top unit] 90 has a public key/private key pair." Furthermore, column 10, lines 46-49, states that "the conditional access authority maintains a public key database with which it is entrusted to ensure that every public key corresponds to the proper STU 90."

Serial No.: 09/743,653  
Customer No. 24498

RCA 89131

From these passages, it can be easily seen that, according to Wasilewski, each set top unit will have a unique public/private key pair, and that the controlling conditional access authority would track which public key was assigned to each set top box. This is contrary to the element of claim 1 where "the private key is shared among a plurality of subscribers." Thus, Wasilewski teaches away from the above cited element of claim 1.

The Applicant further respectfully asserts that the use of individual private keys, as taught by Wasilewski, requires that each broadcast stream sent to each individual set top box be separately encrypted and transmitted. Such separate encryption and transmission requires far greater hardware capacity than that the method recited in claim 1. Accordingly, an artisan skilled in broadcast security would not look to Wasilewski to address the same problems solved by the present principles, as embodied in claim 1.

As amended, claim 1 recites the method step of "decrypting said access information in a conditional access module using a private key associated with the shared public key, *wherein the private key is shared among a plurality of subscribers.*" The present specification, as filed, states, at page 14, lines 32-35, that "There is a global RSA public/private key pair, Kpub/Kpri, for the entire system. The public key is shared by all of the broadcasters, and the corresponding private key is placed in the tamper-proof NRSS-A based smart cards, distributed by the CA providers to the consumers."

The use of private keys by multiple consumers permits broadcasters to encrypt data transmission a single time for a given set of consumers. The requirement of Wasilewski that broadcasters encrypt the broadcast stream for each individual set top box, and the associated greater hardware requirements, is thus eliminated.

The elimination of separate broadcast streams may also be particularly useful in situations where the broadcast bandwidth is limited. According to page 5, lines 19-20 of the present specification, "this invention finds benefit in terrestrial broadcasting."

It would be virtually impossible for the system of Wasilewski to be employed in terrestrial broadcasting. As discussed above, the teachings of Wasilewski require that each individual set top unit have a public/private key pair, where the broadcast stream being sent to each individual set top unit is encrypted for the particular set top unit. Thus, a separate, individual broadcast stream would be required for each set top box. Transmitting an individually encrypted broadcast to each set top unit over terrestrial broadcasting would be impossible, as the sheer volume of transmissions would quickly overwhelm the bandwidth available to a broadcaster.

Serial No.: 09/743,653  
Customer No. 24498

RCA 89131

In contrast to the teachings of Wasilewski, claim 1 recites a method where single broadcasting stream may be accessed by multiple consumers. According to claim 1, multiple consumers receive the same broadcast, which is encrypted with the same public key. The use of a single private key by a plurality of consumers to decrypt the broadcast permits a terrestrial broadcaster to effectively broadcast to an unlimited number of consumers.

Thus, Wasilewski teaches away from the feature of "decrypting said access information in a conditional access module using a private key associated with the shared public key, *wherein the private key is shared among a plurality of subscribers*", and Wasilewski would not be obvious to combine with Kudelski. Even an artisan highly skilled in the art of broadcast security would not be motivated to look to Wasilewski to solve the problems addressed by claim 1. Therefore, Wasilewski fails to render obvious all of the elements of claim 1.

The Examiner has further acknowledged that "Kudelski does not explicitly disclose using a public key system for encrypting the access information, where the public key is shared." (See page 3, first paragraph of the Office Action of February 6, 2007). While Kudelski teaches that any encryption system may be used, the state of the art at the time Kudelski was developed appears to preclude the use of a public key encryption system. Specifically, Kudelski fails to contemplate the mechanics of a public key encryption system where a plurality of consumers share a private key. For example, Kudelski makes no allowance for the distribution of public or private keys. Without a mechanism for distributing at least the public key, Kudelski could not effectively make use of a public key encryption system.

Kudelski fails to teach, or even suggest such a public key encryption scheme recited in the present claims. In particular, Kudelski makes no teaching or suggestion that would lead one skilled in the art to develop a broadcast security system having a public key encryption scheme where "*the private key is shared among a plurality of subscribers*."

Thus, taken singly, or in any combination, Kudelski and Wasilewski fail to teach or suggest at least the method step of "decrypting said access information in a conditional access module using a private key associated with the shared public key, *wherein the private key is shared among a plurality of subscribers*."

MPEP §2143.03 states "To establish *prima facie* obviousness of a claimed invention, all the claim limitations must be taught or suggested by the prior art. *In re Royka*, 490 F.2d 981, 180 USPQ 580 (CCPA 1974). "All words in a claim must be considered in judging the patentability of that claim against the prior art." *In re Wilson*, 424 F.2d 1382, 1385, 165 USPQ 494, 496 (CCPA 1970). If an independent claim is nonobvious under 35 U.S.C. 103, then any claim

Serial No.: 09/743,653  
Customer No. 24498

RCA 89131

depending therefrom is nonobvious. *In re Fine*, 837 F.2d 1071, 5 USPQ2d 1596 (Fed. Cir. 1988)."

Having failed to render obvious at least one element of claim 1, Kudelski and Wasilewski, taken singly, or in any combination, cannot render obvious claim 1 as a whole. The Applicant, therefore, respectfully asserts that claim 1 is patentable over the cited combination of Kudelski and Wasilewski for at least the reasons cited above.

Claims 2-4, 6 and 15-17 depend from independent claim 1. By virtue of their dependencies, claims 2-4, 6 and 15-17 have all of the features and limitations of the independent claims from which they depend. Thus, claims 2-4, 6 and 15-17 are patentable for at least the same reasons as claim 1.

In view of the foregoing, the Applicant respectfully requests that the rejection of the claims set forth in the Office Action of February 6, 2007 be withdrawn, that pending claims 1-4, 6 and 15-17 be allowed, and that the case proceed to early issuance of Letters Patent in due course.

It is believed that no additional fees or charges are currently due. However, in the event that any additional fees or charges are required at this time in connection with the application, they may be charged to the Applicant's Deposit Account No. 07-0832.

Respectfully submitted,

Ahmet Mursit Eskicioglu et al.

By:



Paul Kiel, Attorney for Applicants  
Registration No. 40,677  
(609) 734-6815

Patent Operations  
Thomson Licensing LLC  
P.O. Box 5312  
Princeton, NJ 08543-5312

*August 9, 2007*